

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-025427

(43)Date of publication of application : 27.01.2005

(51)Int.Cl. G06F 15/00
G06F 3/12
G06F 13/00

(21)Application number : 2003-189238

(71)Applicant : TOSHIBA CORP
TOSHIBA TEC CORP

(22)Date of filing : 01.07.2003

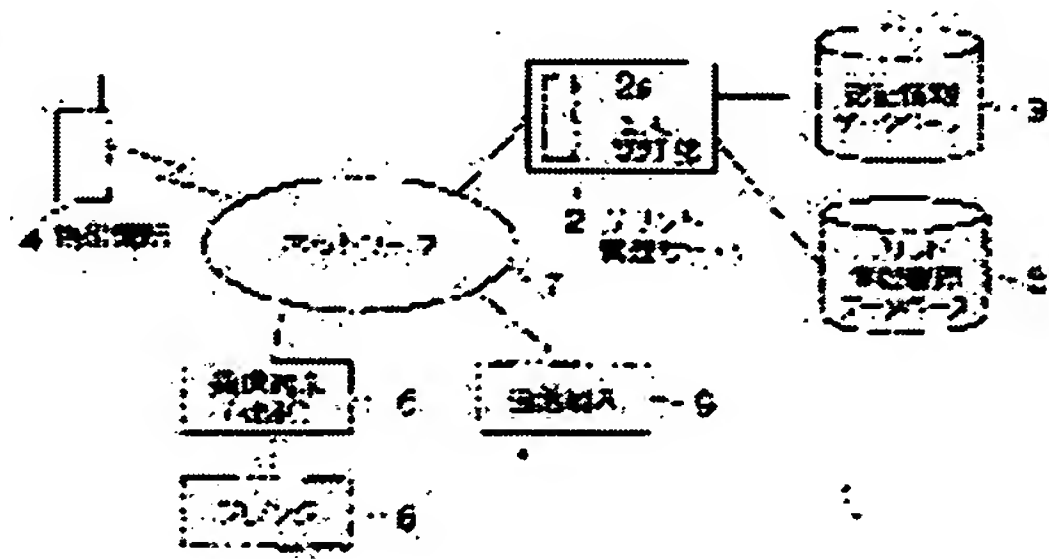
(72)Inventor : KOYAMA SATOSHI

(54) AUTHENTICATION DEVICE AND SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an authentication device and an authentication system releasing locked personal identification information with simple and greatly ensured security.

SOLUTION: This authentication device is provided with a personal information storage means storing individual personal identification information associated with electronic mail addresses of respective registered users, a personal identity authentication means authenticating the personal identity of the registered user, and a lock releasing information creation means creating lock releasing information releasing prohibition individually when the use of the personal identification information is prohibited. The authentication device is also provided with an electronic mail communication means which transmits a lock notification mail carrying a communication address of the lock releasing information and lock releasing identification information at least to the electronic mail address matching the personal identification information, and a lock releasing means receiving access to the communication address of the lock releasing information and performing authentication based on the received lock releasing identification information for releasing the prohibition of the disabled personal identification information.



BEST AVAILABLE COPY

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-25427

(P2005-25427A)

(43) 公開日 平成17年1月27日(2005.1.27)

(51) Int. Cl. ⁷	F 1	テーマコード (参考)
G 0 6 F 15/00	G 0 6 F 15/00 3 3 0 B	5 B 0 2 1
G 0 6 F 3/12	G 0 6 F 3/12 K	5 B 0 8 5
G 0 6 F 13/00	G 0 6 F 13/00 5 4 7 V	
	G 0 6 F 13/00 6 3 0 A	

審査請求 未請求 請求項の数 7 O L (全 14 頁)

(21) 出願番号	特願2003-189238 (P2003-189238)	(71) 出願人	000003078
(22) 出願日	平成15年7月1日(2003.7.1)		株式会社東芝
			東京都港区芝浦一丁目1番1号
		(71) 出願人	000003562
			東芝テック株式会社
			東京都千代田区神田錦町1丁目1番地
		(74) 代理人	100090620
			弁理士 工藤 宜幸
		(74) 代理人	100092576
			弁理士 鎌田 久男
		(72) 発明者	小山 悟史
			東京都港区芝公園2丁目4番1号 秀和芝
			パークビル 東芝テック株式会社内
		Fターム(参考)	5B021 BB00 NN18
			5B085 AE01

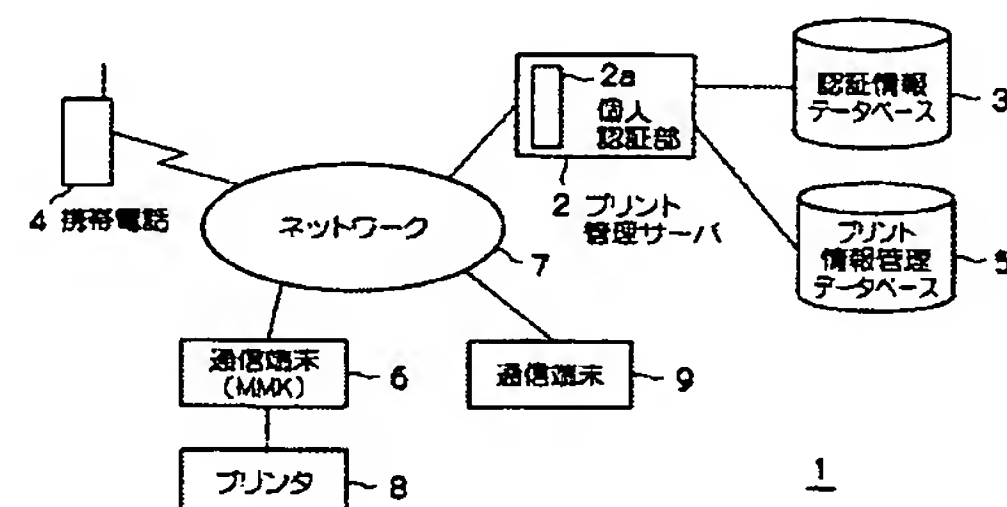
(54) 【発明の名称】 認証装置及び認証システム

(57) 【要約】

【課題】 ロックされた個人識別情報の解除を簡便かつ高いセキュリティで行なう認証装置及び認証システムを提供する。

【解決手段】 本発明の認証装置は、登録ユーザの各個人識別情報に少なくとも各登録ユーザの電子メールアドレスを対応付けて記憶する個人情報記憶手段と、登録ユーザの個人認証を行なう個人認証手段と、個人識別情報が使用禁止とされたときに、その禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、その個人識別情報に対応する電子メールアドレスを送信先とし、少なくともロック解除情報の通信アドレスとロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、ロック解除情報の通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない、使用禁止された個人識別情報の禁止を解除するロック解除手段とを備える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

登録ユーザの各個人識別情報に、少なくとも各登録ユーザのユーザ通信端末の電子メールアドレスを対応付けた個人情報記憶する個人情報記憶手段と、
登録ユーザの個人認証を行なう個人認証手段と、
上記個人認証手段により個人認証の正当性が認められず、個人識別情報が使用禁止とされたときに、当該個人識別情報の禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、
使用禁止となった上記個人識別情報に対応する電子メールアドレスを送信先とし、少なくとも、上記ロック解除情報に割り当てた通信アドレスと、ロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、
上記ロック解除情報に割り当てた通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない正当である場合、使用禁止された上記個人識別情報の禁止を解除するロック解除手段と
を備えることを特徴とする認証装置。

【請求項 2】

上記ロック解除情報作成手段は、上記ロック解除情報の通信アドレスが同時期に重複しない通信先アドレスを割り当てることを特徴とする請求項 1 に記載の認証装置。

【請求項 3】

上記個人認証手段は、
各個人識別情報毎に使用禁止となったロック回数を監視するロック回数監視部と、
所定の監視期間内に所定回数以上のロックがあった個人識別情報とは異なる新しい個人識別情報の作成をする個人識別情報作成手段と、
上記ロック解除手段による解除後、既に登録されている個人識別情報を上記新しい個人識別情報に変更する個人識別情報変更部と
を有することを特徴とする請求項 1 又は 2 に記載の認証装置。

【請求項 4】

上記ロック解除手段は、上記ロック解除情報の通信先アドレスへのアクセス待ち受け期間を設け、その待ち受け期間までにアクセスがない場合、上記ロック解除情報を無効にすることを特徴とする請求項 1 ～ 3 のいずれかに記載の認証装置。

【請求項 5】

上記ロック解除用識別情報が、上記個人認証情報記憶手段に記憶されている個人識別情報及び上記ユーザのみが知るパスワードであることを特徴とする請求項 1 ～ 4 のいずれかに記載の認証装置。

【請求項 6】

上記電子メール通信手段は、上記ロック解除手段による解除後、当該個人識別情報に対応する電子メールアドレスを送信先として、ロック解除が終了した旨のロック解除通知メールを送信することを特徴とする請求項 1 ～ 5 のいずれかに記載の認証装置。

【請求項 7】

少なくとも電子メール手段及び閲覧表示手段を有する登録ユーザの通信端末と、
少なくとも個人識別情報と上記登録ユーザの電子メールアドレスを対応させた個人情報を保管し、ネットワークを介して受信した個人識別情報に基づいて個人認証を行なう請求項 1 ～ 6 のいずれかに記載の認証装置と
を備え、

上記登録ユーザの通信端末は、受信したロック通知メールに記載された上記ロック解除情報の通信アドレス先にアクセスして、上記ロック解除用識別情報を上記認証装置に与えて、個人識別情報の禁止を解除させることを特徴とする認証システム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、認証装置及び認証システムに関し、例えば、ユーザ端末等から指示したコンテンツ情報（ファイル情報）を、コンビニエンスストアや駅などに設置されているマルチメディアキオスク端末（MMK）等をユーザが利用して取得し印刷出力するWebを使用したサービスシステムにおいて、登録ユーザの個人認証を行なう認証装置及び認証システムに適用できる。

【0002】

【従来の技術】

近年、インターネットの利用態様の多様化及び携帯電話等の移動通信端末の多機能化に伴い、インターネットを利用した様々なWebを使用したサービスがある。

【0003】

例えば、ユーザが所持するブラウザ機能を搭載した携帯端末を利用してインターネット上のサーバと通信を行ない所望チケット等を予約購入するシステムについて記載されている（下記特許文献1参照）。また例えば、ユーザ又はその関係者がWebサーバにファイル情報の格納を行ない、ユーザがMMK等を利用して外出先からでもそのWebサーバのファイル情報を呼出し印刷出力するシステムサービスもある。

【0004】

このような様々なWebを使用したサービスをユーザに提供する場合、そのユーザが本人であるか否かの正当性を判断することは重要であり、さまざまな認証方式がある（下記特許文献2参照）。

【0005】

一般的な個人認証方式として、例えば、ユーザに割り当てられたユーザIDと本人しか知らないパスワード等の認証情報を認証装置のデータベースに予め登録しておき、ユーザがサービスを受ける際に、ユーザが移動通信端末やMMK等を利用してユーザID及びパスワードを入力して認証装置に送信し、受信した入力ユーザIDに基づいて、入力パスワードと登録パスワードとの一致・不一致を認証装置が判断することによりユーザの本人認証が行われている。

【0006】

そして、認証装置が、ユーザID及びパスワードの一致と判断した場合、ユーザ本人の正当性を認め、不一致と判断した場合、ユーザ本人ではないと判断する。

【0007】

【特許文献1】

特開2002-215986号公報

【0008】

【特許文献2】

特開2002-259264号公報

【0009】

【発明が解決しようとする課題】

しかしながら、ユーザはサービスを受けるためのユーザID及びパスワードを覚えておく必要があり、ユーザがユーザID及びパスワードを忘れてしまい、何度か連続して間違えたユーザID及びパスワード等を入力試行したにもかかわらず個人認証の正当性が得られなかった場合、認証装置はそのユーザIDを使用禁止にする場合がある。Webサーバが認証装置と連携する場合には、Webサーバによるサービスの提供も行われなくなる。

【0010】

このような場合には、ユーザは、認証装置の運営者側又はサービス提供者側と直接連絡を取り、新たなユーザID等の発行や登録変更等のユーザIDの使用禁止状態を解除する所定の手続が必要であった。

【0011】

また、このようなユーザIDの使用禁止状態を解除する手順を熟知している第三者は、あるユーザの入力ユーザID及び入力パスワードとして適当なものを入力して、ユーザIDを故意に使用禁止状態にした後に、認証装置運営者側又はサービス提供者と連絡を取り、

10

20

30

40

50

新しいユーザIDを取得することで、ユーザになりすましてサービスの提供を受けるといふなりすまし行為が行われるおそれもある。

【0012】

そのため、登録ユーザでないとの認証結果によりサービスが使用禁止状態になった場合に、そのサービス使用禁止状態の解除手続を、登録ユーザにとって利便性が高く、かつ、第三者によるなりすましを防止しより高いセキュリティで行なう認証装置及び認証システムが求められている。

【0013】

【課題を解決するための手段】

かかる課題を解決するために、第1の本発明の認証装置は、(1)登録ユーザの各個人識別情報に、少なくとも各登録ユーザのユーザ通信端末の電子メールアドレスを対応付けた個人情報記憶手段と、(2)登録ユーザの個人認証を行なう個人認証手段と、(3)個人認証手段により個人認証の正当性が認められず、個人識別情報が使用禁止とされたときに、当該個人識別情報の禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、(4)使用禁止となった個人識別情報に対応する電子メールアドレスを送信先とし、少なくとも、ロック解除情報に割り当てた通信アドレスと、ロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、(5)ロック解除情報に割り当てた通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない正当である場合、使用禁止された個人識別情報の禁止を解除するロック解除手段とを備えることを特徴とする。

【0014】

第2の本発明の認証システムは、(1)少なくとも電子メール手段及び閲覧表示手段を有する登録ユーザの通信端末と、(2)少なくとも個人識別情報と登録ユーザの電子メールアドレスを対応させた個人情報を保管し、ネットワークを介して受信した個人識別情報に基づいて個人認証を行なう第1の本発明の認証装置とを備え、登録ユーザの通信端末は、受信したロック通知メールに記載されたロック解除情報の通信アドレス先にアクセスして、ロック解除用識別情報を認証装置に与えて、個人識別情報の禁止を解除させることを特徴とする。

【0015】

【発明の実施の形態】

(A)実施形態

以下、本発明の認証装置及び認証システムの実施形態について図面を参照して説明する。

【0016】

本実施形態は、ユーザ端末等から指示されたファイル情報をプリント管理サーバに格納させ、登録ユーザが、外出先からでもコンビニエンスストアや駅などに設置されているマルチメディアキオスク端末(MMK)等を利用して、プリント管理サーバにアクセスしてファイル情報を取得し印刷出力するWebを使用したシステムに適用した場合を説明する。

【0017】

(A-1)実施形態の構成

図1は、本実施形態の認証システムの全体構成を示すものである。図1に示すように、本実施形態の認証システム1は、プリント管理サーバ2、認証情報データベース3、携帯電話4、プリント情報管理データベース5、コンビニエンスストア等に設置されている通信端末(MMK)6、プリンタ8、ファイル登録を指示する通信端末9を備える。また、ネットワーク7は、公衆網や移動通信網やインターネット等の通信網であり、プリント管理サーバ2と、通信端末6と、携帯端末4と、ファイル登録を指示する通信端末9はネットワーク7を通じて接続可能である。

【0018】

通信端末9は、プリント管理サーバ2にファイル情報の格納指示を行なう通信端末であり、ネットワーク7に接続可能なPCやブラウザ機能を有する携帯電話やMMK等が該当する。

【0019】

プリント管理サーバ2は、通信端末9から登録指示されたファイル情報を、ユーザ毎に割り当てた保管領域に保管するものである。また、プリント管理サーバ2は、通信端末6からの印刷実行時により、保管しているファイル情報を通信端末6に送信するものである。なお、本実施形態では印刷実行する通信端末9をMMKとして説明するが、プリンタデバイスと接続する通信端末であれば広く適用できる。

【0020】

プリント管理サーバ2は、上記のほかに登録ユーザの個人認証処理、ユーザ管理、セキュリティ管理、印刷履歴管理、ファイル情報の印刷等に対する課金管理などを統合的に行なうサーバであり、コンテンツ情報の印刷サービスの提供をするものである。

10

【0021】

プリント管理サーバ2は、認証処理時は、印刷実行時に通信端末6からのユーザID及びパスワードに基づいて認証処理を行なうものである。

【0022】

プリント管理サーバ2は、ファイル情報の登録時に、ユーザの個人認証処理を行わず、プリント管理サーバ2が発行したアドレスに対して、例えば、通信端末9からファイル情報を添付した電子メールを送信することで、アドレス（保管領域）にファイル情報を登録することができる。

【0023】

また、プリント管理サーバ2は、プリント情報管理データベース5におけるファイル情報の格納位置情報と、登録ユーザによりファイル情報を呼出するための印刷識別情報とをユーザIDに対応させて管理し、外部から受信した印刷識別情報や個人識別情報に基づいて格納されたファイル情報や個人情報をネットワーク7を通じて送信するものである。

20

【0024】

プリント情報管理データベース5は、登録ユーザにより指示されたファイル情報を格納するデータベースである。

【0025】

次に、プリント管理サーバ2の個人認証部2aについて、図2を参照して説明する。

【0026】

図2に示すように、個人認証機能2aは、制御部21が実行するソフトウェアで構成され、通信部22と、ユーザ登録機能部23と、個人認証機能部24と、ロック解除機能部25とを有する。

30

【0027】

制御部21は、プリント管理サーバ2の個人認証機能を制御するものである。

【0028】

ユーザ登録機能部23は、Webを使用したサービスの提供を受けるユーザの個人情報を認証情報データベース3に登録・保存し、図3に示す認証情報管理テーブルを有して登録ユーザの認証情報を管理するものである。

【0029】

認証情報管理テーブルは、図3に示すように、プリント管理サーバ2側が各登録ユーザを識別するために付与したユーザIDに、少なくとも、サーバあるいはユーザが決定したパスワード（例えば、最初はサーバ側が決定したパスワードを発行し、その後ユーザにより決定できるパスワードを含む）、電子メールアドレス、所定の監視期間内に発生した総ロック回数、ロック発生時に付与されるロックフラグを対応させ記憶するものである。勿論、他の項目として、ユーザの氏名・住所、電話番号や年齢その他の個人情報、認証履歴等を記憶するようにしてもよい。

40

【0030】

ここで、電子メールアドレスは、登録ユーザ本人に電子メールを送信するために必要であり、ユーザが所持する電子メール機能を有する携帯電話4の電子メールアドレスや、ユーザが所有するPCの電子メールアドレス等を示す。本実施形態ではユーザが所持する携帯

50

電話 4 の電子メールアドレスとする。

【0031】

また、登録するパスワードや電子メールアドレスの数を複数個としても良い。また、ユーザ登録機能部 23 は、登録ユーザの意思に基づいて、認証情報データベース 3 に保存した個人情報の内容を変更・追加・削除できるようにしてもよい。この場合、既に登録されているユーザ ID 及びパスワードによる個人認証処理後に行なうことが好ましい。

【0032】

例えば、ユーザの電子メールアドレスを変更する場合、登録ユーザの個人認証の正当性を判断した後、ユーザ登録機能部 23 は、登録ユーザの操作による通信端末 9 からのユーザ ID に対応する個人情報を認証情報データベース 3 から取り出し、新しい電子メールアドレスに上書き修正したり、又は、登録電子メールアドレスを削除して新しい電子メールアドレスを再登録する等して変更できるようにしてよい。また、個人情報の内容の追加についても、個人情報の内容の変更と同様にしてするようにしてよい。また、個人情報の内容の削除は、個人情報の一部又は全部を削除するようにしてもよい。

【0033】

個人認証機能部 24 は、Web を使用したサービスの提供前に、Web を使用したサービスの利用希望者にユーザ ID 及びパスワードの入力要求後、その入力ユーザ ID 及びパスワードに基づいて、ユーザの個人認証を行なうものである。

【0034】

個人認証機能部 24 は、受信したユーザ ID に基づいて認証情報データベース 3 に登録されている個人情報を取り出し、その対応する登録パスワードと入力パスワードとが一致するか否かを判断して認証するものであり、入力パスワードと登録パスワードとが一致する場合、登録ユーザ本人であることを認め、また入力パスワードと登録パスワードとが不一致である場合、登録ユーザ本人でないと判断する。

【0035】

個人認証が NG の場合、個人認証機能部 24 は、通信端末 9 に対して所定回数（例えば 3 回）の再試行の機会を要求してもよい。また、この再試行によっても個人認証が NG である場合は、登録ユーザでないと判断し、そのユーザ ID を使用不可能な状態に（ロック）する。ユーザ ID のロックは、例えば、そのユーザ ID に対応する個人情報にロックした旨のフラグをたてて、フラグがたててあるユーザ ID については使用不可能であるものと し、認証情報データベース 3 に保存するようにする。

【0036】

また、個人認証機能部 24 は、ロックされたユーザ ID に対応する個人情報から総ロック回数を監視し、総ロック回数が所定の監視期間内で所定回数（例えば 3 回）以上である場合、新たなユーザ ID を準備（確保）する。

【0037】

個人認証機能部 24 は、登録されているユーザ ID を新しいユーザ ID に変更し、既に登録されているユーザの個人情報を新しいユーザ ID に対応させて認証情報データベース 3 に保存する。

【0038】

この総ロック回数の監視期間及び総ロック回数は、認証装置 2 の管理者側が、例えば、時分、日、月、年等の単位で自由に設定できる。また、登録ユーザが、登録時又は登録後に、この監視期間及び総ロック回数を指定できるようにしてもよい。

【0039】

ロック解除機能部 25 は、個人認証機能部 24 によりユーザ ID がロックされると、そのロックされたユーザ ID のロックを解除するためのファイル情報を作成し、そのファイル情報をロック解除用サイトとした URL (Uniform Resource Locator) を作成する。

【0040】

このロック解除用サイトは、ユーザ ID のロック発生につき、そのユーザ ID に対応する

URLが割り当てられて作成されるものであって、そのURLは、他のロック解除用サイトのURLと同時期に重複しないものである。ロック解除用サイトは、例えば、1個のユーザIDに対応する1個のURLを発行し、その後のユーザIDのロック発生後にも、同一のURLを使用させることができる。また、各ロック発生毎に異なるURLを作成させるようにしてもよい。

【0041】

また、ロック解除機能部25は、ロック解除サイト作成後、ロックされたユーザIDに対応する電子メールアドレスを送信先として、ロック解除用サイトのURLと、ユーザID及びパスワードとをメール内容に記載した電子メール（ロック通知メール）を送信する。登録された電子メールアドレスにロック通知メールを送信することで、正確に登録ユーザ 10
に通知することができる。

【0042】

なお、ロック通知メールに、プリント管理サーバ2の管理者側の電話番号やユーザIDのロック発生の年月日時等やその他情報も記載するようにしてもよい。

【0043】

ロック解除機能部25は、ユーザIDのロック解除が終了すると、割り当てられたURLを無効にする。

【0044】

ロック解除機能部24は、ロックされたユーザIDについてのロック解除が終了すると、ロック通知メールを送信した送信先と同様の電子メールアドレス（登録ユーザの登録電子 20
メールアドレス）に、ロックが解除された旨のロック解除通知メールを送信する。

【0045】

ロック解除用サイトでは、ロック通知メールを携帯電話4で受信したユーザが利用する通信端末（例えばMMK6、ユーザの通信端末9等を含む）から、電子メールに記載のURLに基づいてアクセスされ、電子メールに記載のユーザID及びパスワードの入力送信要求をその通信端末に行なう。ロック解除用サイトでは、受信したパスワードと登録パスワードとの一致・不一致を判断して、一致する場合には、そのユーザIDのロックを解除し、不一致の場合にはユーザIDのロックを維持する。不一致の場合には、所定回数の再試行を要求してもよい。また、ユーザは、可能であれば、ブラウザ機能を有する携帯電話2 30
からロック解除用サイトにアクセスできるようにしてもよい。

【0046】

通信部22は、通信ボードや通信ソフトウェア等が該当し、ネットワーク7の通信を可能にする通信機能及び電子メール通信機能を有するものである。

【0047】

図1に戻り、通信端末6は、コンビニエンスストアや駅などに設置されているマルチメディアキオスク端末等が該当し、図6に示すように、ユーザ操作部61、情報通信部62、画面表示部63、一時的に情報を記憶する記憶部64、制御部65、プリンタ制御部66などを有するものである。

【0048】

また、通信端末6は、ユーザの操作により、ネットワーク7を通じてプリント管理サーバ 40
2からファイル情報を取得し、接続するプリンタ8からファイル情報を出力するものである。

【0049】

携帯電話2は、Webブラウザ機能及び電子メール機能を有する携帯電話であり、ユーザの操作により、認証装置2とアクセスし得るものである。携帯電話4は、Webブラウザ機能により、認証装置2が有するコンテンツを閲覧可能であり、認証装置2からの要求に応じてユーザID及びパスワード等の入力及び送信するものである。また、携帯電話4は、電子メール機能により、認証装置2から電子メールを受信可能であり、その電子メールに添付されたロック解除用サイトのURLをユーザに知らせるためのものである。

【0050】

(A-2) 実施形態の動作

次に、本実施形態の認証装置及び認証システムの動作について説明する。

【0051】

以下では、プリント管理サーバ2による個人認証部2aの個人認証処理、ユーザIDのロック動作及びロックされたユーザIDのロック解除動作について詳細に説明する。

【0052】

なお、登録ユーザのユーザID、パスワード及び電子メールアドレスを少なくとも含む個人情報、認証情報データベース3に予め登録されていることを前提として説明する(S1)。

【0053】

まず、プリント管理サーバ2のサービスの提供を受けようとする者(保管ファイル情報の印刷実行する者)の操作により、通信端末(MMK)6はプリント管理サーバ2の個人認証部2aにアクセスする(S2)。なお、以下では、プリント管理サーバ2へのアクセスを通信端末(MMK)6によるものとして説明するが、これに限らずユーザがサービス利用を行なう際に利用する通信端末(例えば図1の通信端末9)であれば広く適用できる。

【0054】

通信端末(MMK)6において、ユーザID及びパスワードが、希望者の操作により入力され、入力されたユーザID及びパスワードが通信端末(MMK)6から個人認証部2aに送信される(S3)。

【0055】

通信端末(MMK)6からのユーザID及びパスワードは個人認証部2aに受信され(S4)、個人認証部2aにおいて、受信したユーザIDに対応するユーザのパスワードが認証情報データベース3から取り出され、受信したパスワードと登録されているパスワードとの一致・不一致が判断される(S5)。

【0056】

パスワードが一致する場合、ユーザが登録ユーザ本人であるとして認証動作を終了し(S6)、プリント管理サーバ2のサービスを受けることが可能となる。

【0057】

個人認証がNGの場合、ユーザID及びパスワードの連続試行回数を検知し(S7)、その試行回数が所定回数未満である場合には、通信端末(MMK)6に対して、ユーザID及びパスワードの再試行入力を通信端末(MMK)6に要求する(S8)。

【0058】

この再試行入力要求に応じて、希望者の操作により、通信端末(MMK)6からの再度ユーザID及びパスワードの入力・送信が行われ、上述したS3～S7の動作が繰り返される。

【0059】

個人認証部2aにより検知された試行回数が所定回数以上である場合、当該ユーザIDが使用不可能に(ロック)される(S9)。

【0060】

ユーザIDをロックする方法として、例えば、そのユーザIDに対応する個人情報のうち、ロックしたことを示すフラグをたてて、このフラグがあるユーザIDについては使用不可能とするように、認証情報データベース3に保存する。

【0061】

また、個人認証部2aにより、ロックがある毎にユーザIDに対応する個人情報のうち総ロック回数が更新される(S10)。ここで、総ロック回数が所定監視期間内に所定回数未満であると個人認証部2aが判断した場合、総ロック回数をクリアしてもよい。

【0062】

個人認証部2aにおいて、総ロック回数が監視され(S11)、所定監視期間内の総ロック回数が所定回数(例えば3回)以上であると判断された場合、当該ユーザIDに代えて新しいユーザIDを発行するために、新しいユーザIDが準備される(S12)。なお、

10

20

30

40

50

新しいユーザIDは、ユーザによるロック解除要求の後で発行されるようにしてもよいし、新しいユーザIDの発行をユーザに問い合わせ希望する場合にのみ発行されるようにしてもよい。

【0063】

新しいユーザIDが準備された後、ロックされたユーザIDのロックを解除するためのロック解除用サイトが作成される（S13）。

【0064】

また、S11に戻り、総ロック回数が所定回数未満であると判断された場合は、新しいユーザIDの準備はされずに、ロック解除用サイトが作成される（S11及びS13）。

【0065】

このロック解除用サイトは、ユーザIDのロック発生につき、そのユーザIDに対応するURLが割り当てられて作成されるものであって、そのURLは、他のロック解除用サイトのURLと同時期に重複しないものである。

【0066】

個人認証部2aにより、認証情報データベース3からロックされたユーザIDに対応する個人情報を取り出され、登録されているユーザの電子メールアドレスを送信先として、今回のロックにつき作成されたロック解除用サイトのURL、登録されているユーザID及びパスワードが、電子メール内容として記載されたロック通知メールが作成され送信される（S14及びS15）。登録された電子メールアドレスにロック通知メールを送信することにより、当該システム利用が、悪意ある第三者であっても、ロックの登録ユーザ本人にのみ通知できる。

【0067】

ロック通知メールが送信された後は、ロック解除用サイトは、ユーザによる携帯電話4からのロック解除要求の受け付けるべく待機状態となる（S16）。

【0068】

次に、ロック通知メールを受信したユーザの要求によりユーザIDのロックを解除する動作について図5を参照して説明する。

【0069】

上述したように、個人認証部2aは、ロック通知メールを送信後、ロック解除用サイトへのアクセスによるユーザのロック解除要求があるまで、ロック解除要求の待機状態となる（S21）。

【0070】

ユーザの操作により、ロック通知メールに記載のロック解除用サイトのURLにアクセスする（S22）。この場合に、ユーザがロック解除用サイトにアクセスするための通信端末6は、ユーザが利用可能な通信端末であれば広く適用でき、例えば、通信端末9、通信端末（MMK）6、ブラウザ機能を有する携帯電話4等を適用するようにしてもよい。

【0071】

例えば、ユーザが外出時にロック通知メールを携帯電話4で受信した後、その受信した位置に近接する通信端末（MMK）6を利用してロック解除用サイトにアクセスしたり、また例えば、会社内にいる場合には、会社でユーザが使用するパソコン（通信端末9）からアクセスするようにしてもよい。

【0072】

なお、以下では、ユーザがロック解除用サイトにアクセスする通信端末を通信端末（MMK）6として説明する。

【0073】

ロック解除用サイトにアクセスした後、ユーザに対しロック通知メールに記載のユーザID及びパスワードを入力するよう要求し、この要求に応じて、ユーザの操作により、ユーザが利用した通信端末6からロック通知メールに記載のユーザID及びパスワードが入力され個人認証部2aのロック解除用サイトに送信される（S23）。このとき、ユーザの意思により、ユーザの個人情報（例えばパスワード等）の変更を個人認証部2aが受け付

10

20

30

40

50

けるようにしてもよい。

【0074】

個人認証部2aのロック解除用サイトにおいて、ユーザが利用した通信端末6からのユーザID及びパスワードを受信し(S24)、ロック解除用サイトに対応付けられたユーザID及びパスワードが正しいか否かが判断される(S25)。

【0075】

ロック解除用サイトによりユーザID及びパスワードが正しくないと判断された場合、そのまま当該ユーザIDのロックは維持される(S26)。このとき、ユーザID及びパスワードの入力について所定回数の再試行を要求できるようにしてもよい。

【0076】

ロック解除用サイトによりユーザID及びパスワードが正しいと判断された場合、個人認証部2aが準備する新しいユーザIDが存在するか否かを確認する(S27)。

【0077】

これは、ロックされたユーザIDについて、新しいユーザIDを発行して登録するのか否かを確認するためである。

【0078】

勿論、新しいユーザIDをユーザのロック解除要求の後で発行する場合には、ロック解除用サイトによるユーザID及びパスワードの認証後又はユーザのユーザIDの発行要求後、新しいユーザIDの発行動作が加わり、新しいユーザIDの存在確認動作は行われない。

【0079】

個人認証部2aにおいて、新しいユーザIDが準備されている場合には、新しいユーザIDとユーザの個人情報とを対応させて認証情報データベース3に保存し、新しいユーザIDの有効性を確保する(S28)。

【0080】

このとき、ロックされたユーザID及びそのユーザIDに対応させた個人情報を削除するようにしてもよいし、又はこのユーザIDの使用不可能な情報にしたまま認証情報データベース3に保持するようにしてもよい。

【0081】

新しいユーザIDの発行後、ユーザの個人情報を対応させた新しいユーザIDを認証情報データベース3に登録することで、新しいユーザIDを有効にしロックを解除する(S29)。

【0082】

S27に戻り、新しいユーザIDが準備されていない場合には、ロックされたユーザIDに対応する個人情報のフラグを削除することでロックを解除する(S27及びS29)。

【0083】

ユーザIDのロック解除終了後、当該ロック発生時に作成したロック解除用サイトのURLを無効にする(S30)。ロック解除用サイトのURLを無効にする時期は、これに限られず、例えば、ロック解除通知メールをユーザの携帯電話4に送信後に無効にしてもよい。

【0084】

ユーザIDのロック解除終了後、当該ユーザIDに対応するユーザの電子メールアドレスを送信先として、ロック解除が終了した旨のロック解除通知メールを作成し、送信する(S31及びS32)。

【0085】

個人認証部2aからロック解除通知メールを受信したユーザは、ユーザIDのロックが解除した旨を知り、既存のユーザID又は新しいユーザIDを用いることで個人認証を行なうことができる(S33)。

【0086】

(A-3) 実施形態の効果

10

20

30

40

50

以上、本実施形態によれば、認証処理時に、少なくともユーザのみが知るパスワード及びユーザの電子メールアドレスを予め登録し、ユーザIDのロック発生時に、ユーザの電子メールアドレスを送信先として、ロック解除用サイトのURL、ユーザID及びパスワードを記載した電子メールを送信することで、登録したユーザにのみ正確にユーザIDのロックの旨及びユーザID及びパスワードの確認をさせることができると共に、登録したユーザのみの操作により、ロック解除用サイトにアクセスしユーザIDのロック解除処理を行なわせることができる。その結果、第三者によるなりすましを防止することができる。

【0087】

また、本実施形態によれば、ユーザにとって負担が少ないロック解除処理でロック解除を行なわせることができる。

10

【0088】

(B) 他の実施形態

(B-1) 上述した実施形態では、ユーザが所持する携帯電話を利用して個人認証する場合について説明したが、携帯電話に限らず、PDAやPHS等その他の移動通信端末やパソコンや店舗に設置されたMMK等の通信端末等広く適用できる。

【0089】

また、携帯端末4に与えられたロック通知メール及びロック解除通知メールを、通信端末(MMK)6に転送できるようにしてもよい。このとき、個人認証部2aは、携帯端末4の位置情報(例えば基地局5から割り出した情報やGPSを利用した緯度経度情報等)を確認し、その位置情報周辺の1又は複数の通信端末(MMK)6を特定し、その特定した公共通信端末(MMK)6でのみ転送指定できるようにしてもよい。

20

【0090】

また、ユーザにWebを使用したサービスを提供するWebサーバ又はシステムが、上述した認証装置及び認証システムを利用することができる。このとき、上述した認証装置及び認証システムは、Webサーバ又はシステム自身が含む装置としてよいし、又はWebサーバ又はシステムとは異なる装置としてもよい。

【0091】

(B-2) 上述した実施形態において、ロック解除用サイトによるユーザIDのロック解除は、ロック通知メールに記載のユーザID及びパスワードの認証により行なうこととして説明したが、これに限らず、例えば、ロック解除機能部25が発行したロック解除用キーをロック通知メールに添付し、ロック解除キーのユーザ入力に基づいてロック解除できるようにしてもよい。

30

【0092】

この場合、ロック解除用キーの発行は、ロック解除用サイトの作成時に、ロック解除機能部25が発行し、当該ユーザIDとロック解除用キーとを対応させて保存することにより認証するようにする。

【0093】

また、ロック通知メールにユーザID及びパスワードを記載することとしたが、ユーザの個人情報登録時に、これらユーザID及びパスワードをロック通知メールに記載するか否か、又は、ロック通知メールに記載する内容をユーザに選択できるようにしてもよい。

40

【0094】

(B-3) 上述した個人認証部2aは、図5のS21~S24でロック解除用サイトの解除要求の受付期限を設定するようにしてもよい。例えば、この解除要求の受付期限を、ロック通知メールの送信日から所定期間(例えば1週間、6ヶ月、1年等設定できる)内と設定し、その期間内にユーザからの解除要求がない場合には、ロックされたユーザIDのロック解除は行われないうようにしてもよい。この場合、個人認証部2aはロック解除用サイトのURLを無効にしたり、又は、当該ユーザIDに対応する個人情報を削除したりしてもよい。

【0095】

(B-4) 上述した実施形態の変形例として、ロック解除用サイトのURLを記載せず、

50

ロックした旨を記載した第1のロック通知メールをユーザの携帯電話4に送信し、まずユーザに電子メールの返信を求めるようにしてもよい。

【0096】

そして、個人認証部2aがユーザからの電子メール返信を確認した後に、ロック解除用サイトのURLを記載した第2のロック通知メールをユーザの携帯電話4に送信するようにしてもよい。

【0097】

また、第1のロック通知メールに対して返信されたユーザの返信電子メールにより、ユーザがロック解除要求、及び又は、新しいユーザIDの発行要求をするようにしてもよい。

【0098】

(B-5) また、上述した実施形態では、ロック発生したユーザID専用のロック解除サイトを作成することとしたが、これに限ることなく、ロック発生したユーザIDを所有する全てのユーザ共通のロック解除サイトを作成するようにしてもよい。

【0099】

例えば、上記共通ロック解除サイトを認証装置2が有するホームページ上に表示し、ロック通知メールを受信したユーザが、上記ホームページ上の共通ロック解除サイトにアクセスして、自身のユーザIDのロック解除を行なうようにしてもよい。

【0100】

この場合、ロック解除機能部25が、ユーザIDのロック発生時に、当該ユーザID専用のロック解除用キーを発行し、そのロック解除用キーをロック通知メールに添付してユーザに送信する。そして、ユーザからの解除要求の際に、ユーザ入力されたロック解除用キーに基づいて、ロック解除用サイトが認証するようにしてもよい。

【0101】

【発明の効果】

以上、本発明によれば、登録ユーザのみがロック通知メールを受信することができ、ロック通知メールを受信した登録ユーザのみが個人識別情報のロックを容易に解除することができる。その結果、第三者による成りすましを防止することができる。

【図面の簡単な説明】

【図1】 実施形態の認証システムの全体構成を示す図である。

【図2】 実施形態の認証装置2の機能構成を示す図である。

【図3】 実施形態の認証情報データベース3が保存する認証情報の項目例を示す説明図である。

【図4】 実施形態の認証装置2の動作を説明するフローチャートである。

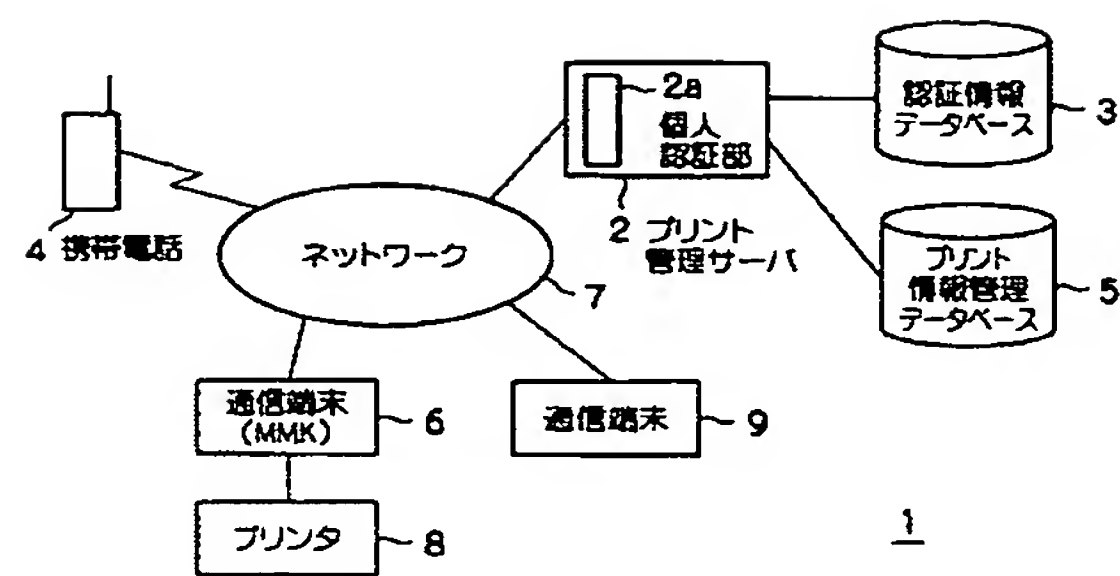
【図5】 実施形態の認証装置2の動作を説明するフローチャートである。

【図6】 実施形態の通信端末6の内部構成を示す図である。

【符号の説明】

1…認証システム、2…プリント管理サーバ、2a…個人認証部、
3…認証情報データベース、4…携帯電話、21…制御部、22…通信部、
23…ユーザ登録機能部、24…個人認証機能部、25…ロック解除機能部。

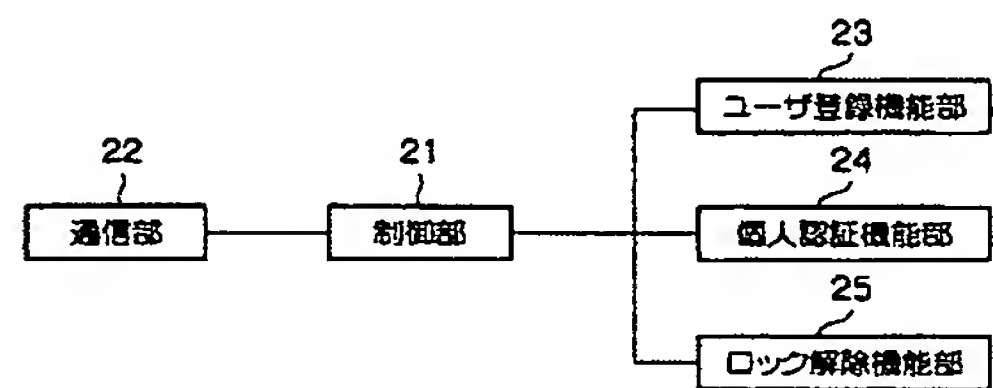
【図 1】



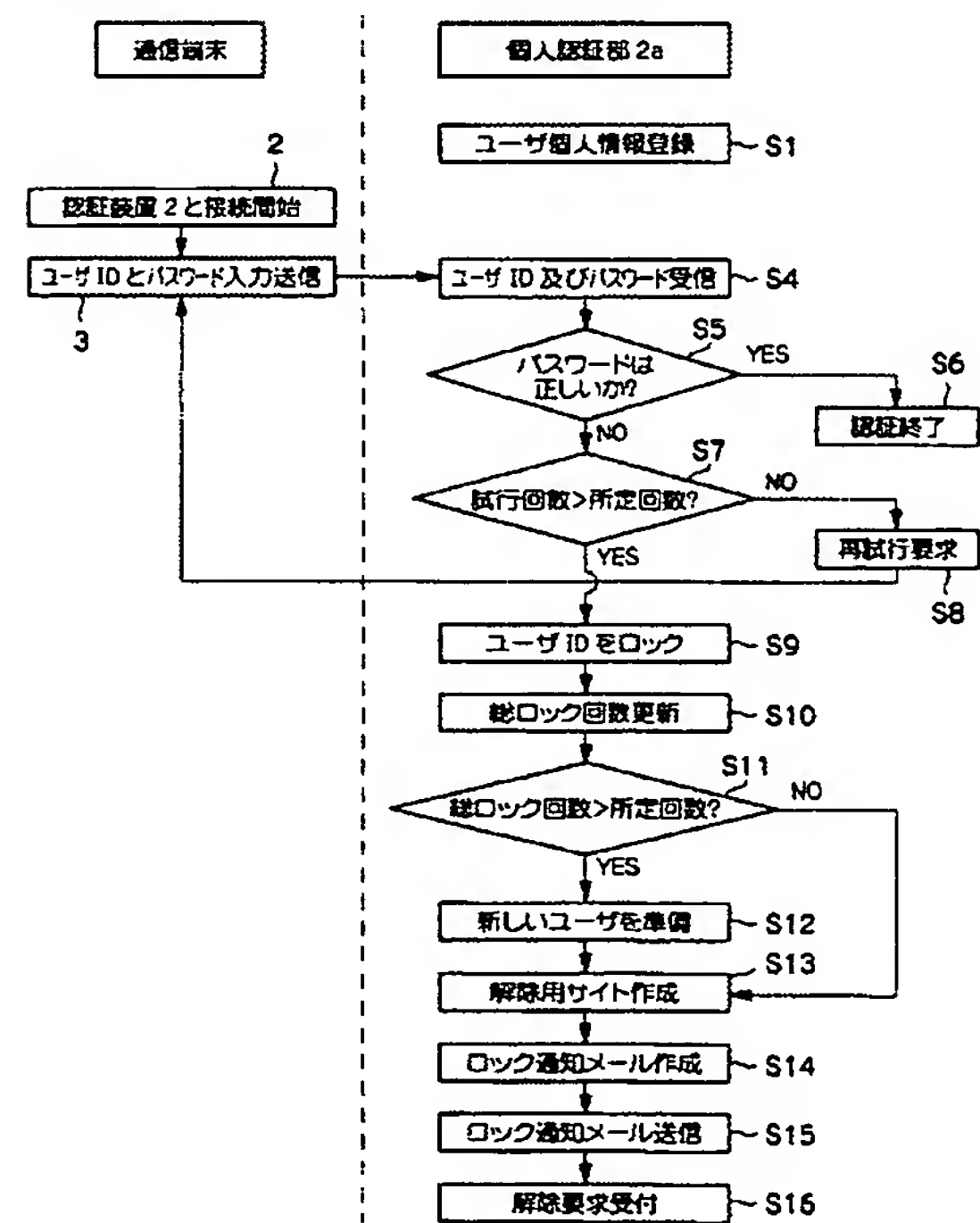
【図 3】

ロックフラグ	✓
総ロック回数	3
電子メールアドレス	yama0000xxx kawa0000***
パスワード	yamamoto kawa0102 ...
ユーザID	101011 101013 ...

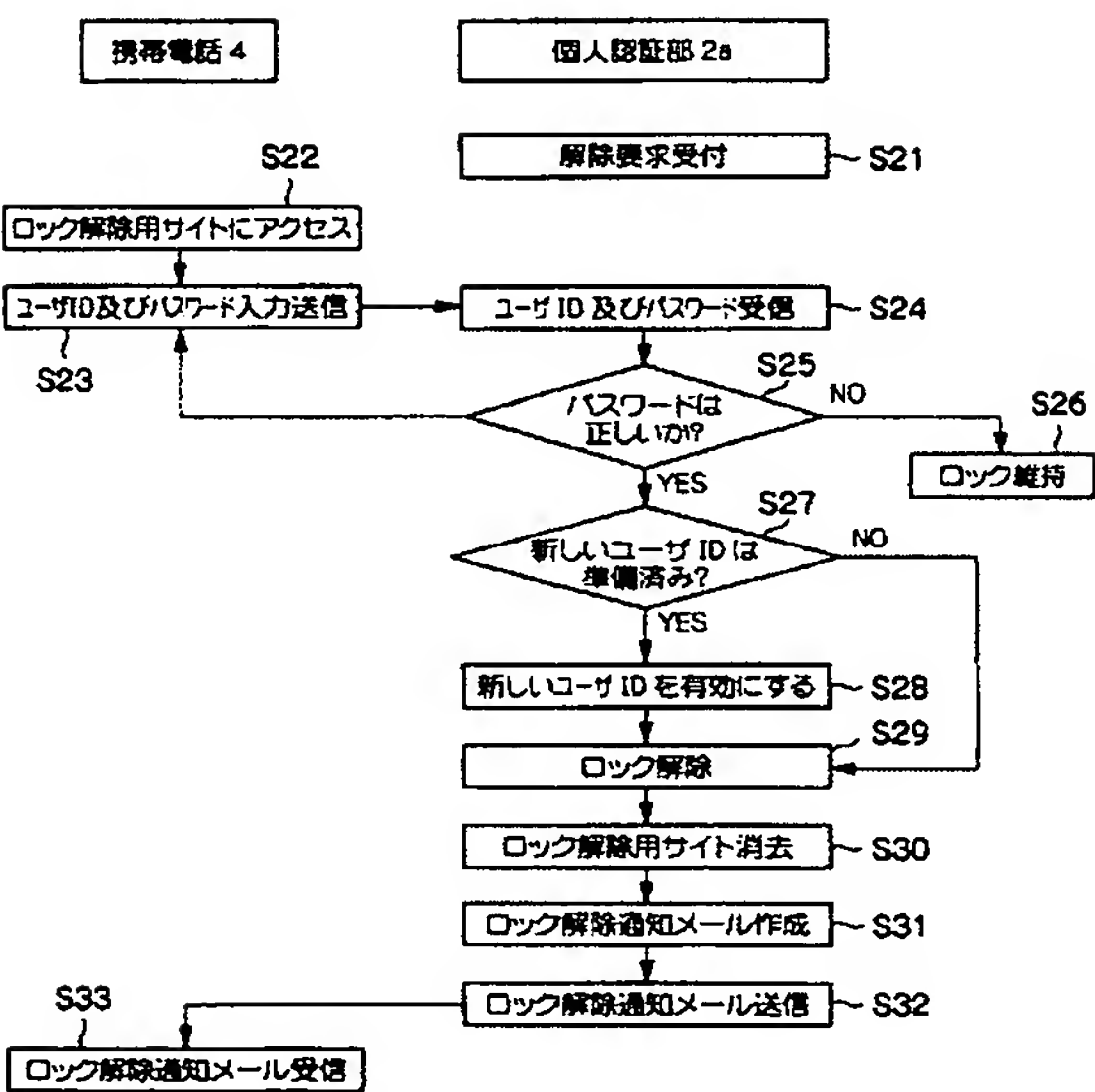
【図 2】



【図 4】



【図 5】



【図 6】

